REPUBLIQUE DU CAMEROUN
Paix – Travail – Patrie

AGENCE NATIONALE DES TECHNOLOGIES DE L'INFORMATION ET DE LA COMMUNICATION

Centre d'Alerte et de Réponse et
Aux Incidents de Sécurité Informatique

REPUBLIC OF CAMEROON
Peace – Work – Fatherland

NATIONAL AGENCY FOR INFORMATION AND COMMUNICATION TECHNOLOGIES

Computer Incident Response Team

Bulletin de sécurité N°2 du mois de Mars 2019

B.P. 6170 Tél : 22 08 64 98 Fax : 22 20 39 29 Web : http//www.antic.cm ; Email : infos@antic.cm

Sommaire

I. LEXIQUE DU BULLETIN

Expression	Signification
Date de publication	Date à laquelle la vulnérabilité a été officiellement publiée par le développeur ou constructeur de la ressource concernée.
Dernière version	Lien de téléchargement de la dernière version de la ressource concernée, dans le cas d'une ressource logicielle ou système d'exploitation.
Description	Présentation des détails sur la vulnérabilité, entre autre les versions de la ressource concernée par la vulnérabilité, le vecteur d'exploitation de la vulnérabilité (local, réseau …).
Référence CVE	CVE (Common Vulnerabilities and Exposures) est un annuaire de vulnérabilités de sécurité. Cet annuaire est maintenu par l'organisme MITRE, soutenu par le Département de la Sécurité intérieure des États-Unis. Les identifiants CVE sont des références de la forme CVE-AAAA-NNNN (AAAA est l'année de publication et NNNN un numéro incrémenté). Plus d'information à l'adresse : http://cve.mitre.org/
Score CVSS	CVSS (Common Vulnerability Scoring System) est un système d'évaluation des vulnérabilités qui permet d'associer une valeur (comprise entre 0 et 10) évaluant la criticité d'une vulnérabilité. CVSS fournit un cadre commun pour évaluer les niveaux de criticité, les caractéristiques et les impacts des vulnérabilités de sécurité informatique. Plus d'informations à aux adresses : http://www.first.org/cvss/cvss-guide.html, http://www.cert-ist.com/fra/ressources/Publications_ArticlesBulletins/Veilletechnologique/CVSSv2/
Solution	Lien vers d'éventuelles solutions permettant de colmater ou de contourner la vulnérabilité.
Vulnérabilité	Faille de sécurité publiée, Synopsis de la faille, généralement sur la forme « Vulnérabilité dans X » où X est une ressource informatique, matérielle, logicielle ou système d'exploitation concernée par la vulnérabilité.

II. Vulnérabilités publiées

II.1 Navigateurs

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans Mozilla Firefox	De multiples vulnérabilités ont été découvertes dans Mozilla Firefox. Elles permettent à un attaquant de provoquer un problème de sécurité non spécifié par l'éditeur, une atteinte à l'intégrité des données et une atteinte à la confidentialité des données. Les versions concernées sont les suivantes : Firefox versions antérieures à 66.0.1	26/03/2019	CVE-2019-9813	66.0.1 Télécharger	Mettre à jour le navigateur	10.0

II.2 SYSTÈMES D'EXPLOITATION

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Fin de support de Windows 7	Microsoft annonce la fin du support de toutes les versions de Windows 7 à partir du 14 janvier 2020. Après cette date les systèmes fonctionnant sous Microsoft Windows 7 ne recevront plus le support technique, les mises à jour et les correctifs de sécurité. Il est recommandé aux différents organismes de planifier la migration des postes utilisateurs utilisant ce système vers une version supportée de Microsoft Windows. Il est à noter que sans mises à jour de sécurité pour le système d'exploitation, vos postes utilisateurs deviennent vulnérables à une panoplie d'attaques qui peuvent cibler les informations contenues dans ces postes ou être utilisés comme porte d'entrée pour attaquer des composants de votre système d'information. Pour plus d'informations sur ce sujet veuillez-vous référer à ce bulletin de Microsoft : - https://support.microsoft.com/fr-ma/help/4057281/windows-7-support-will-end-on-january14-2020					
Vulnérabilité dans Google Chrome OS	De multiples vulnérabilités ont été découvertes dans Google Chrome OS. Elles permettent à un attaquant de provoquer un problème de sécurité non spécifié par l'éditeur. Les versions infectées sont les suivantes : Google Chrome OS versions antérieures à 73.0.3683.88 (Platform version: 11647.104.0/1/2/3)	26/03/2019	CVE-2018-18445	73.0.3683.88 Télécharger	Veuillez-vous référer au Bulletin de sécurité https://chromereleases.googleblog.com/2019/03/stable-channel-update-for-chrome-os_25.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+GoogleChromeReleases+%28Google+Chrome+Releases%29	10.0

Vulnérabilité dans le noyau Linux de SUSE	De multiples vulnérabilités ont été découvertes dans le noyau Linux de SUSE. Certaines d'entre elles permettent à un attaquant de provoquer un déni de service, un contournement de la politique de sécurité et un problème de sécurité non spécifié par l'éditeur. Les systèmes infectés sont les suivants : • SUSE Linux Enterprise Workstation Extension 12-SP4 • SUSE Linux Enterprise Software Development Kit 12-SP4 • SUSE Linux Enterprise Server 12-SP4 • SUSE Linux Enterprise Live Patching 12-SP4 • SUSE Linux Enterprise High Availability 12-SP4 • SUSE Linux Enterprise Desktop 12-SP4 • SUSE Linux Enterprise Live Patching 12-SP3 • SUSE Linux Enterprise Module pour Live Patching 15	27/03/2019	CVE-2019-8980	Contacter SUSE	Veuillez-vous référer au Bulletin de sécurité https://www.suse.com/support/update/announcement/2019/suse-su-20190767-1/	10.0

II.3 CMS

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans le CMS Drupal	Une vulnérabilité a été découverte dans Drupal. Elle permet à un attaquant de provoquer une injection de code indirecte à distance (XSS). Les versions affectées sont les suivantes : • Drupal 8.6.x versions antérieures à 8.6.13 • Drupal versions antérieures à 8.5.14 • Drupal 7.x versions antérieures à 7.65	21/03/2019	–	8.6.13 Télécharger	Mettre à jour le CMS	8.5

II.4 AUTRES

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans Moodle	De multiples vulnérabilités ont été découvertes dans Moodle. Elles permettent à un attaquant de provoquer un problème de sécurité non spécifié par l'éditeur, un contournement de la politique de sécurité et une élévation de privilèges. Les systèmes affectés sont les suivants : • Moodle versions 3.6 à 3.6.2 • Moodle versions 3.5 à 3.5.4 • Moodle versions 3.4 à 3.4.7 • Moodle versions 3.1 à 3.1.16 et versions antérieures non supportées	19/03/2019	CVE-2019-3852	3.6.2 Contacter Moodle	Veuillez-vous référer au guide de sécurité pour obtenir les correctifs https://moodle.org/mod/forum/discuss.php?d=384015	7.3

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans PuTTY	De multiples vulnérabilités ont été découvertes dans PuTTY. Certaines d'entre elles permettent à un attaquant de provoquer une exécution de code arbitraire, un déni de service et un problème de sécurité non spécifié par l'éditeur. Les systèmes infectés sont les suivants : • PuTTY toutes versions antérieures à 0.71	22/03/2019	CVE-2019-9898	0.71 Télécharger	Veuillez-vous référer au guide de sécurité pour obtenir les correctifs https://www.chiark.greenend.org.uk/~sgtatham/putty/wishlist/	5.2
Vulnérabilité dans Tenable Nessus	De multiples vulnérabilités ont été découvertes dans Tenable Nessus. Elles permettent à un attaquant de provoquer un déni de service et une atteinte à la confidentialité des données. Les systèmes affectés sont les suivants : • Nessus 8.2.3 et versions antérieures	27/03/2019	CVE-2019-18214	8.3.0 Contacter Nessus	Veuillez-vous référer au guide de sécurité pour obtenir les correctifs https://www.tenable.com/security/tns-2019-02	3.1

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans Cisco IP Phone	De multiples vulnérabilités ont été découvertes dans Cisco IP Phone. Certaines d'entre elles permettent à un attaquant de provoquer une exécution de code arbitraire à distance, un déni de service à distance et un contournement de la politique de sécurité. Les systèmes affectés sont les suivants : • Cisco IP Phone exécutant une version logicielle de SIP antérieure à 11.0(5) pour Wireless IP Phone 8821-EX et 12.5(1)SR1 pour la série IP Phone 8800 • Cisco IP Phone 7800 et 8800 exécutant une version logicielle de SIP avec la fonctionnalité web service active antérieure à 10.3(1)SR5 pour Unified IP Conference Phone 8831, 11.0(4)SR3 pour Wireless IP Phone 8821 et 8821-EX et 12.5(1)SR1 pour le restes des IP Phone 7800 et 8800	21/03/2019	CVE-2019-1766	Contacter CISCO	Veuillez-vous référer au guide de sécurité pour obtenir les correctifs https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190320-ip-phone-csrf	4.3

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans les produits Apple	De multiples vulnérabilités ont été découvertes dans les produits Apple. Certaines d'entre elles permettent à un attaquant de provoquer une exécution de code arbitraire, un déni de service et un contournement de la politique de sécurité. Les versions vulnérables sont : • Apple iOS versions antérieures à 12.2 • Apple macOS Mojave versions antérieures à 10.14.4 • Apple macOS High Sierra sans le correctif de sécurité 2019-002 • Apple macOS Sierra sans le correctif de sécurité 2019-002 • Apple tvOS versions antérieures à 12.2 • Apple Safari versions antérieures à 12.1 • Apple iTunes pour Windows versions antérieures à 12.9.4 • Apple iCloud pour Windows versions antérieures à 7.1 • Apple Xcode versions antérieures à 10.2	26/03/2019	CVE-2019-8567	Contacter Apple	Veuillez-vous référer au bulletin de sécurité https://support.apple.com/en-us/HT209606	6.2

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans Magento	De multiples vulnérabilités ont été découvertes dans Magento. Certaines d'entre elles permettent à un attaquant de provoquer une exécution de code arbitraire, un contournement de la politique de sécurité et une atteinte à l'intégrité des données. Les systèmes infectés sont les suivants : • Magento Open Source versions antérieures à 1.9.4.1 • Magento Commerce versions antérieures à 1.14.4.1 • Magento 2.1 versions antérieures à 2.1.17 • Magento 2.2 versions antérieures à 2.2.8 • Magento 2.3 versions antérieures à 2.3.1	27/03/2019	–	Contacter Magento	Veuillez-vous référer au bulletin de sécurité https://magento.com/security/patches/supee-11086	5.3

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans Mozilla Thunderbird	De multiples vulnérabilités ont été découvertes dans Mozilla Thunderbird. Elles permettent à un attaquant de provoquer un problème de sécurité non spécifié par l'éditeur, une atteinte à l'intégrité des données et une atteinte à la confidentialité des données. Les systèmes infectés sont les suivants : Mozilla Thunderbird versions antérieures à 60.6.1	26/03/2019	CVE-2019- 9813	60.6.1 Télécharger	Veuillez-vous référer au bulletin de sécurité https://www.mozilla.org/en-US/security/advisories/mfsa2019-12/	6.3

III. ACTUALITÉS

1. Des chercheurs découvrent 36 failles dans les réseaux 4G

Un groupe de chercheurs de l'université Korea Advanced Institute of Science and Technology (KAIST) a analysé deux réseaux 4G opérationnel et y a découvert 36 failles de sécurité. Certaines sont générales, car liées au design du standard. D'autres proviennent d'une mauvaise implémentation technique et sont donc spécifiques à un opérateur.

https://www.01net.com/actualites/des-chercheurs-ont-decouvert-36-failles-dans-des-reseaux-4g-1660751.html

2. Asus reconnait avoir été la cible d'un piratage sophistiqué

Le fabricant informatique Asus vient de publier un communiqué dans lequel il admet avoir été la cible d'une attaque sophistiquée, que Kaspersky avait dévoilée il y a deux jours sous le nom de ShadowHammer. La firme taïwanaise publie un correctif de Live Update, le logiciel de mise à jour que les pirates ont utilisé pour diffuser une porte dérobée sur des centaines de milliers d'ordinateurs de la marque.

https://www.01net.com/actualites/asus-reconnait-avoir-ete-la-cible-d-un-piratage-sophistique-et-publie-un-patch-1660599.html

3. Ils ont hackés la Tesla model 3 et sont repartis avec

Succès sur toute la ligne pour les hackers Amat Cama et Richard Zhu, qui ont fait équipe sous le nom « Fluoroacetate » à l'occasion du concours de piratage Pwn2Own. Celui-ci s'est déroulé il y a quelques jours à Vancouver. Les deux chercheurs ont décroché le prix de la catégorie « Automobile » en piratant une Tesla Model 3. Grâce à une faille dans le compilateur JIT du navigateur web intégré, ils ont réussi à exécuter du code au niveau du système de divertissement de la voiture électrique, au travers d'un site web vérolé. Cet exploit leur a permis de gagner une récompense de 35.000 dollars. Ils ont également pu garder le véhicule, ce qui rajoute une valeur de plus de 35.000 dollars.

https://www.01net.com/actualites/ils-ont-hacke-la-tesla-model-3-et-sont-repartis-avec-1659160.html

4. Les faiblesses du système de chiffrement de Windows

Le chercheur Denis Andzakovic de Pulse Security a réussi à extraire la clé utilisée par le système de chiffrement BitLocker de Microsoft, présent dans les versions professionnelles de Windows 10. Pour cela, il a connecté un « renifleur » (sniffer en anglais) à la puce de sécurité TPM (Trusted Platform Module) d'une tablette Surface Pro 3. Ce circuit stocke la clé VMK (volume master key), mais elle est ensuite transmise « en clair » lors du démarrage de l'ordinateur.
https://www.01net.com/actualites/un-chercheur-revele-les-faiblesses-du-systeme-de-chiffrement-de-windows-10-1657412.html

5. Infiltration du site officiel de la Commission Européenne

Des pirates dans Europa.eu ! Voilà qui va beaucoup amuser les propagandistes politiques de tout poil. Alors que l'on ne cesse d'entendre parler des « Fakes News », de manipulation de l'information à des fins politiciennes. Actions menées par des pirates Russes, Américains, d'extrême droite, d'extrême gauche… c'est oublier que la majorité des fausses « news » sont mises en ligne par des black marketeurs. Des professionnels de la manipulation marketing

https://www.zataz.com/infiltration-du-site-officiel-de-la-commission-europeenne-europa-eu/

6. Acheter de l'or des diamants et des faux billets sur le black market

Avez-vous déjà entendu parler des « Diamants de sang » ? Saviez-vous qu'il est très compliqué de connaître le nom de la mine d'or d'où a été extrait le minerai qui a permis de créer la chaîne que vous avez autour du cou ; de la bague que vous avez au doigt. Pour les diamants de sang, des pierres précieuses venues de Centre Afrique. Terre de guerre prise en main par des milices armées qui utilisent les mines pour financer armes et munitions. Des diamants interdits à la vente.

https://www.zataz.com/acheter-de-lor-des-diamants-ou-des-faux-billets-dans-le-black-market/

7. Plan de reprise après une attaque

Si les sinistres IT sont par définition imprévisibles, la restauration des données ne devrait pas l'être. Elle devrait au contraire être planifiée, prévisible et contrôlée. Voici quelques recommandations pour développer une stratégie pour un plan de reprise après sinistre au cohérent avec le fonctionnement de votre entreprise.

https://www.undernews.fr/reseau-securite/neuf-etapes-pour-elaborer-un-plan-de-reprise-apres-sinistre-adapte.html

IV. NOTES IMPORTANTES

1. Veuillez enregistrer les adresses alerts@antic.cm et alerts@cirt.cm parmi vos contacts ou l'enregistrer comme expéditeur approuvé afin de ne plus recevoir les mails en provenance de cette adresse dans vos spam.
2. Ce document est produit régulièrement et téléchargeable sur notre site web www.cirt.cm . Vous y trouverez aussi des alertes et autres publications relatives à la cybersécurité et à la cybercriminalité.
3. Microsoft annonce la fin du support de toutes les versions de Windows 7 à partir du 14 janvier 2020. Après cette date les systèmes fonctionnant sous Microsoft Windows 7 ne recevront plus le support technique, les mises à jour et les correctifs de sécurité. Il est recommandé aux différents Organismes de planifier la migration des postes utilisateurs utilisant ce système vers une version supportée de Microsoft Windows, notamment en prenant en compte cette migration dans les prévisions budgétaires.

   https://support.microsoft.com/fr-ma/help/4057281/windows-7-support-will-end-on-january14-2020
4. Windows XP SP3 et Office 2003 ne sont plus supportés depuis le 8 avril 2014 par Microsoft. Si votre organisation n'a pas encore effectué une migration vers un poste de travail moderne, votre système d'information court de grands risques. En se basant sur les données des déploiements passés des clients Microsoft, le déploiement moyen en entreprise peut prendre de 18 à 32 mois. Pour plus d'informations :
   http://www.microsoft.com/fr-fr/windows/enterprise/fin-support-XP/default.aspx

   L'utilisation des solutions ne possédant aucun support technique présente un risque élevé étant donné qu'aucun correctif ne sera émis après d'éventuelles vulnérabilités détectées sur celles-ci.
5. Afin de se prémunir au maximum d'éventuelle attaques informatiques pouvant endommager tout ou partie de vos systèmes, vous devez mettre à jour tous vos systèmes et logiciels utilisés. Nous vous recommandons donc de télécharger et d'installer toutes les dernières versions de logiciels et systèmes utilisés, uniquement sur les sites des constructeurs. Car tout logiciel téléchargé d'une source autre que celle du constructeur est potentiellement compromise par des malware et chevaux de Troie.

   Par ailleurs, si vous rencontrez quelques difficultés que ce soit dans l'application des correctifs susmentionnés ou ailleurs vous pouvez nous contacter à travers les adresses email alerts@antic.cm et alerts@cirt.cm ou au numéro de téléphone **242 09 91 64**.